WEB APPLICATION FIREWALL MANAGEMENT

FortiWeb Manager Administration Guide

VERSION 5.4.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, December 08, 2015

FortiWeb Manager 5.4.1 Administration Guide

1st Edition

TABLE OF CONTENTS

Introduction 4
- Using FortiWeb Manager to configure devices 4
- Web UI organization 5

What's new 6

Installation 8
- Software requirements 8
- Uploading the license 8

Accessing the web UI 10

System settings 11
- Status 11
- HA 11
  - HA requirements 11
  - HA settings 12
  - HA Status 14
- Users 14
- Logs 15
  - Package Install 15
  - Templates Assign 15
  - Event 16

Add, configure, and provision devices (Device Manager tab) 17
- Add a group 17
- Add a device 17
- Access device configuration 18
- Creating and applying provisioning templates 19

Create and install reusable server policies (Policy & Objects tab) 21
- Package installation 21
- Editing packages 21

Introduction

FortiWeb Manager centralizes the configuration of FortiWeb appliances. Its web UI replaces the local interfaces on FortiWeb appliances in your network, allowing you to create, deploy and update their configurations remotely.

Instead of creating a local configuration on a remote FortiWeb, the manager allows you to create a configuration that you can install on one or more FortiWebs. To make changes to a configuration, edit the FortiWeb Manager package (or create a new one) and deploy the updated package to the remote appliance.

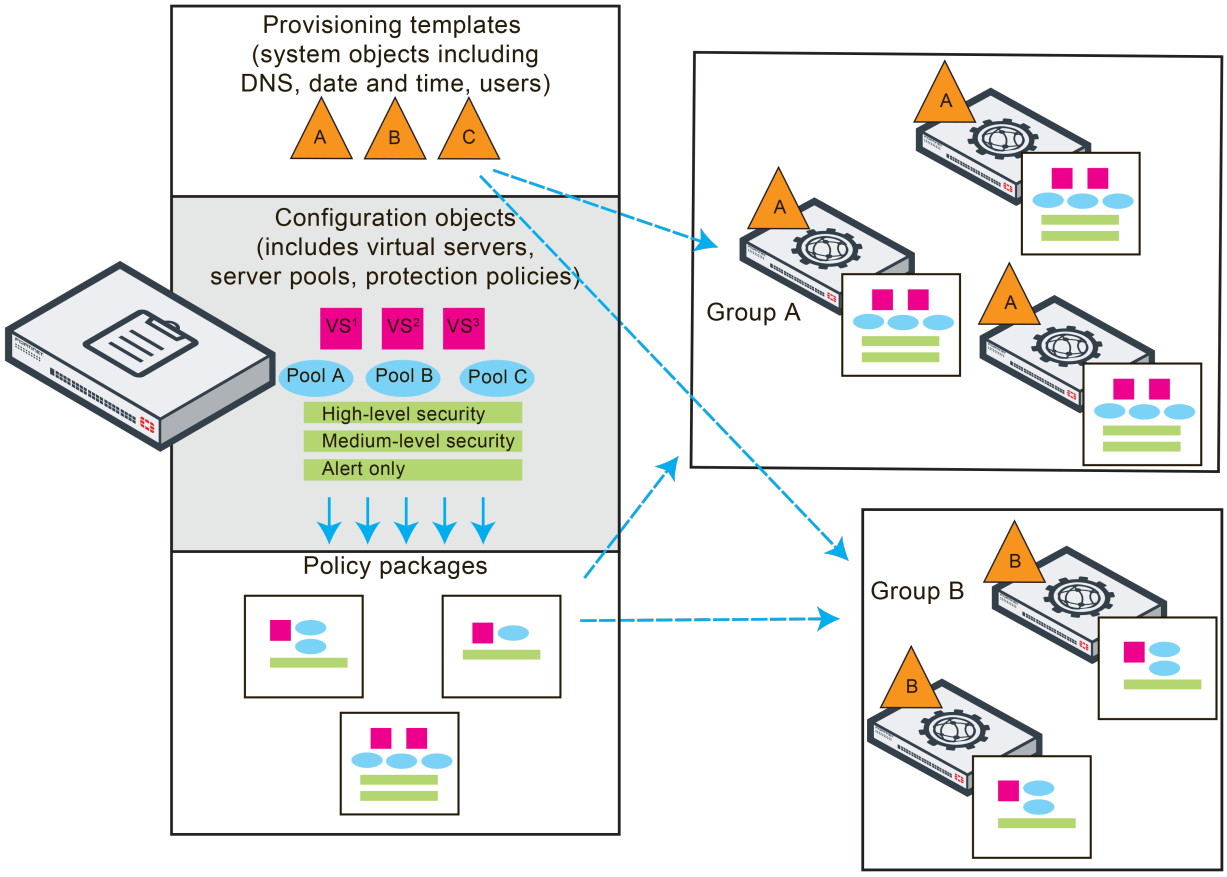
The configuration you install using FortiWeb Manager replaces any default or existing configuration on the remote appliance. However, you can revert to the previous configuration using the installation logs. (See Package Install on page 15 and Templates Assign on page 15.

Using FortiWeb Manager to configure devices

In FortiWeb Manager, FortiWeb configuration is organized in two parts:

- **Provisioning templates** – System objects including DNS, SNMP, and security settings. In most cases, you set these settings during an initial deployment and do not update them often.
- **Policy packages** – Contain one or more policies you create using configuration objects such as virtual servers, server pools, and web protection policies. You create these configuration objects separately and add them to the policies found in packages as needed.

  To update configurations you installed using policy packages, edit the configuration objects and policies as needed, and then install the updated package.



Web UI organization

You perform tasks that configure remote FortiWeb devices using the following two tabs:

- **Device Manager tab** – Allows you to perform the following provisioning tasks:
  - Create a list of FortiWeb appliances available for configuration. To help you organize your devices, you can add a device to a group when you add it.
  - Change an individual configuration setting on an appliance.
  - Create and assign reusable system templates that contain values for the settings that are most commonly used when you provision an appliance, including DNS, SNMP, and security settings.
- **Policy & Objects tab** – Allows you to perform the following policy creation and installation tasks:
  - Create configuration objects such as virtual servers, server pools, and web protection profiles.
  - Create or update policy packages. You create the package policies using the pre-built configuration objects.
  - Install the policy packages on one or more FortiWeb appliances.

The FortiWeb Manager web UI also has a **System Settings tab** that allows you to monitor FortiWeb Manager and to perform tasks such as user management and high availability configuration.

What's new

The list below contains new or changed features for FortiWeb Manager version 5.4 and later.

FortiWeb Manager 5.4.1

- **High Availability** — You can group multiple FortiWeb Manager VM appliances together as a high availability (HA) cluster. HA for FortiWeb Manager uses the same configuration settings as HA for FortiWeb appliances, except for the physical port monitoring options.

  See HA on page 11.

- **FortiWeb 5.4.1 support** — FortiWeb Manager supports all new and enhanced functionality introduced with FortiWeb 5.4.1.
  - **SNMP version 3 support** — When you use the Device Manager tab to configure an SNMP community, you can now enable the traps for SNMP v3 instead or in addition to SNMP v1 and v2c.
  - **Policy Sessions widget** — The Policy Sessions widget on the Status dashboard now displays counts of the current connections and connections per second by policy.
- **Real Time Monitor widget** — You can now view the Real Time Monitor widget when you use the Device Manager tab to access a remote appliance's Status Dashboard.
- **Logging**
  - **Template assign and package install logs** — The new logs generate an entry each time you assign a template or install a package. Each entry includes a record of the previous configuration and information such as the template or package name, the device name, and the time of installation. You can use this entry to revert to the previous configuration or download the current or previous installation for troubleshooting purposes.

    See Package Install on page 15 and Templates Assign on page 15.

  - **Event Log** — On the System Settings tab, go to **Logs > Event** to view a record of user actions such as login, logout, add or delete user, and change password.

    See Event on page 16.

- **3000E & 4000E support** — FortiWeb Manager now supports the additional settings used by the FortiWeb 3000E and 4000E models.

FortiWeb Manager 5.4

- **FortiWeb Manager-VM** — The standalone FortiWeb Manager-VM replaces the central management component that was available in some earlier releases of FortiWeb.

  This new central management tool is not available as an appliance-based product and does not include FortiWeb.
- **Enhanced web UI** — The new web UI has tabs and specialized menus that divide management tasks into provisioning, individual setting updates, and policy creation and installation.
- **Device management tab** — The new Device Manager tab allows you to organize your FortiWeb appliances into groups, change individual appliance configuration settings, and provision a FortiWeb by creating and applying a template.

- **Policy & Objects tab** — The new Policy & Objects tab allows you to upload the FortiWeb policies using reusable packages. You create these packages using configuration objects such as virtual servers, server pools, and web protection profiles. You can create, save, and update both the packages and the objects as needed, and install or reinstall them as needed to apply the policies to multiple devices.
- **Cascading and right-click menus** — When you select an appliance on the Device Manager tab, you can use the **Menu** option to open a cascading menu. This menu allows you to navigate to a specific set of configuration settings quickly. You can right-click device, device group, and policy items in the navigation tree to add new items.
- **Base and unlimited licenses** — New licenses remove the 15-day limit of the evaluation license and allow you to manage either 10 or an unlimited number of FortiWeb devices.

Installation

Currently, FortiWeb Manager is available only as a version of FortiWeb-VM that you can deploy on a VMware vSphere ESXi hypervisor.

For detailed instructions for installing the FortiWeb Manager virtual machine, see the *FortiWeb-VM Installation Guide*.

Software requirements

FortiWeb Manager manages devices running FortiWeb 5.4.1 only.

The web UI works with the following browser versions:

- Internet Explorer 10 or 11
- Firefox 25 or 26
- Chrome 26, 30, 31

Uploading the license

By default, FortiWeb Manager is installed with an evaluation license that allows you to configure 1 FortiWeb.

To continue to use the product after 15 days have passed, or to configure additional gateways, one of the following licenses is required. Neither license has an expiry date:

- **Base** – Add up to 10 devices.
- **Unlimited** – No limit to the number of devices you can add.

You upload the base and unlimited licenses using the CLI. For instructions for configuring access to the CLI, see the *FortiWeb-VM Installation Guide*.

To upload a FortiWeb Manager license

1. Log in to the CLI using admin and enter the following command:

   ```
   generate computerid
   ```

2. FortiWeb returns a 16-character code. For example:

   ```
   3FFWH-QS01H-8TVEW-CN6JE
   ```

3. Go to support.fortinet.com and log in.
4. Click **Asset > Register/Renew**.
5. Enter your license registration code, and then click **Next**.
6. Enter the computer ID you generated earlier, and then click **Next**.

7. Complete any remaining steps in the registration wizard.

   The wizard generates a license key. For example:

   ```
   66KW6E7PHP2BPN6TDI4W83V7S9ZV182EITMZ5NOAE2ZMZDISW5Y2GVIV4UE8NU4Q
   ```

8. Log in to the CLI using admin and enter the following command:

   ```
   execute register license <license_key>
   ```

   where `<license_key>` is the key provided by the support site.

   After the virtual machine restarts automatically, full FortiWeb Manager functionality is available.

Accessing the web UI

Accessing the FortiWeb Manager web UI is similar to accessing the FortiWeb web UI: in your web browser, enter the IP address of the network interface that you have configured with administrative access .

For detailed instructions for configuring access to the web UI, see the *FortiWeb-VM Installation Guide*.

System settings

You use the System Settings tab to monitor FortiWeb Manager and to perform tasks such as user management and high availability configuration.

Status

The system status dashboard has some of the same widgets as the FortiWeb web UI.

Like the FortiWeb dashboard, on the System Information widget, you can click **Update** to upload a new version of the FortiWeb Manager firmware.

HA

You can group multiple FortiWeb Manager appliances together as an **active-passive** high availability (HA) cluster. HA for FortiWeb Manager uses the same configuration settings as HA for FortiWeb appliances, except for the physical port monitoring options.

FortiWeb Manager HA is **active-passive**: one appliance is the active appliance (also called the primary, main, or master) and the other appliance is a passive standby (also called the secondary, or slave), which assumes the role of the active appliance only if the active appliance fails.

This guide provides basic information about the FortiWeb Manager HA settings. See the *FortiWeb Administration Guide*for detailed HA cluster information, including:

- An overview of HA heartbeat & synchronization mechanisms and behavior
- How HA chooses the active appliance
- HA cluster topology
- Step-by-step configuration
- Troubleshooting

HA requirements

- Two identical FortiWeb Manager appliances (that is, VMs running the same firmware version).
- A valid license for all cluster members. You cannot configure HA with trial licenses.
- vNetwork interfaces that carry heartbeat and synchronization traffic are configured to operate in promiscuous mode and accept MAC address changes.
- Cluster members have the same number of ports and are configured with the same amount of memory and vCPUs.
- Redundant network topology: if the active appliance fails, physical network cabling and routes can redirect web traffic to the standby appliance.
- At least one port on both HA appliances is connected directly, via crossover cables, or through switches.

HA settings

Setting name	Description
Configured HA mode	Select **Active-Passive** to configure this FortiWeb Manager to an HA cluster.
Group-name	Enter a name that identifies the HA pair. This setting is optional, and does not affect HA function. The maximum length is 35 characters.
Device Priority	Type the priority for this appliance when the HA feature selects the main appliance in the HA pair. The appliance with the lowest value has the highest priority. This setting is optional. The valid range is 0 to 9. The default is 5. When **Override** is disabled, uptime is more important than this setting when the HA feature selects the primary appliance.
Override	Enable to make **Device Priority** a more important factor than uptime when the HA feature selects the main appliance.
HA Member Group ID	Enter a number that identifies the HA pair. **Ensure that both members of the HA pair have the same group ID.** If there is more than one HA pair on the same network, ensure each HA pair has a different group ID. Changing the group ID changes the cluster's virtual MAC address. The valid range is 0 to 63. The default value is 0.
Detection Interval	Enter the number of 100-millisecond intervals in each pause between heartbeat packets that the one cluster member sends to the other member. This is also the amount of time that a FortiWeb Manager appliance waits before expecting to receive a heartbeat packet from the other appliance. The HA feature synchronizes this setting between the main appliance and standby appliance. The valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds). **Note:** Although this setting is synchronized between the main and standby appliances, configure both appliances with the same **Detection Interval** to prevent a failover from occurring before the initial synchronization.

Setting name	Description
Heartbeat Lost Threshold	Enter the number of times one of the HA appliances retries the heartbeat and waits to receive HA heartbeat packets from the other HA appliance before it assumes that the other appliance has failed. The HA feature synchronizes this part of the configuration between the main appliance and standby appliance. In most cases, you do not need to change this setting. Exceptions include: • Increase the failure detection threshold if the HA feature detects a failure when none has actually occurred. For example, during peak traffic times, if the main appliance is very busy, it might not respond to heartbeat packets in time, and the standby appliance assumes that the main appliance has failed. • Reduce the failure detection threshold or detection interval if administrators and HTTP clients have to wait too long before they can connect through the main appliance, resulting in noticeable down time. The valid range is from 1 to 60. **Note:** Although this setting is synchronized between the main and standby appliances, configure both appliances with the same **Heartbeat Lost Threshold** to prevent a failover before the initial synchronization.
ARP Packet Numbers	Enter the number of times that the FortiWeb Manager appliance broadcasts extra address resolution protocol (ARP) packets when it takes on the main role. (Even though a new NIC has not actually been connected to the network, FortiWeb Manager does this to notify the network that a new physical port has become associated with the IP address and virtual MAC of the HA pair.) This is sometimes called “using gratuitous ARP packets to train the network,” and can occur when the main appliance is starting up, or during a failover. Also configure **ARP Packet Interval**. In most cases, you preserve the default value for this setting. Exceptions include: • Increase the number of times the main appliance sends gratuitous ARP packets if your HA pair takes a long time to fail over or to train the network. Sending more gratuitous ARP packets can help the failover to happen faster. • You want reduce the amount of traffic produced by a failover. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair still fails over successfully, you could reduce the number of times gratuitous ARP packets are sent. The valid range is 1 to 16.

Setting name	Description
ARP Packet Interval	Enter the number of seconds the HA feature waits between each broadcast of ARP packets. In most cases, you preserve the default value of this setting. Exceptions include: • Decrease the interval if your HA pair takes a long time to fail over or to train the network. Sending ARP packets more frequently can help the failover to happen faster. • You want reduce the amount of traffic produced by a failover. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair still fails over successfully, you could reduce the number of times gratuitous ARP packets are sent. The valid range is from 1 to 20.
Heartbeat Interface	Select one or more ports on this appliance that the main and standby appliances use to send heartbeat signals and synchronization data to each other (that is, the HA heartbeat link). Connect this port to the same port number on the other member of the HA cluster. For example, if you select **port3** for the primary heartbeat link, connect port3 on **this** appliance to port3 on the **other** appliance.) Select at least one heartbeat interface on each appliance in the HA cluster. You cannot re-use ports that currently have an IP address assigned for other purposes as a heartbeat link. **Tip:** If enough ports are available, you can select both a primary heartbeat interface and a secondary heartbeat interface on each appliance in the HA pair to provide heartbeat link redundancy. (You cannot use the same port as both the primary and secondary heartbeat interface on the same appliance, as this is incompatible with the purpose of link redundancy.) **Note:** If a switch is used to connect the heartbeat interfaces, the heartbeat interfaces must be reachable by Layer 2 multicast.

HA Status

To determine which appliance currently has the role of the main appliance, on the System Settings tab, click **Status**. The **System Information** widget displays whether the appliance is operating as the main or standby appliance.

Users

Click **System Settings > Users** to access the following user management tasks:

- Add a user
- Edit user information (including passwords)

Logs

Package Install

Each time you install a policy package to a device, FortiWeb Manager adds a new entry to the Package Install log. You can use this log to undo the package installation or download a copy of the current or previous configuration for troubleshooting or backup.

Whenever you install a package, FortiWeb Manager performs a complete backup of the existing configuration. This configuration is the Original Configuration in the Package Install log.

Column name	Description
Package Name	The name of the package in FortiWeb Manager.
Device Name	The name of the device where the package was installed.
Install Time	The time that the package was installed.
Log Name	Click the value to download the configuration that FortiWeb Manager installed.
Original Configuration	Click the value to download the configuration that FortiWeb Manager replaced with the policy package specified by **Log Name**.
Comment	Displays any comment you added when you installed the policy package.
Action	Click **Revert** to re-install the configuration that FortiWeb Manager backed up (saved as the Original Configuration file) before it installed the new policy package. Click **Delete** to remove this entry from the **Package Install** log.

Templates Assign

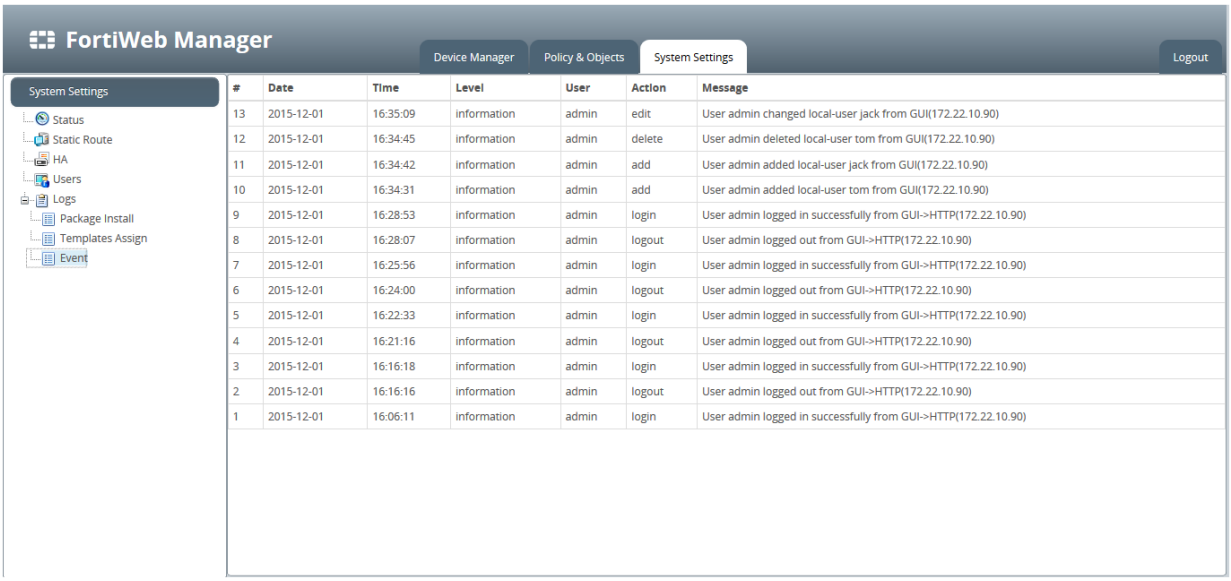
Each time you assign a system template to a device, FortiWeb Manager adds a new entry to the Templates Assign log. You can use this log to undo the template assignment or download a copy of the current or previous settings for troubleshooting or backup.

Whenever you assign a template, FortiWeb Manager performs a complete backup of the existing configuration. This configuration is the Original Configuration in the Templates Assign log.

Column name	Description
Template Name	The name of the system template in FortiWeb Manager.
Device Name	The name of the device the template was assigned to.
Assign Time	The time that the template was assigned.
Log Name	Click the value to download the template that FortiWeb Manager assigned.
Original Configuration	Click the value to download the configuration that FortiWeb Manager replaced with the template specified by **Log Name**.
Action	Click **Revert** to revert to the template configuration values that FortiWeb Manager backed up (saved as the Original Configuration file) before it assigned the new template. Click **Delete** to remove this entry from the **Templates Assign** log.

Event

On the System Settings tab, go to **Logs > Event** to view a record of user actions such as login, logout, add or delete user, and change password.



#	Date	Time	Level	User	Action	Message
13	2015-12-01	16:35:09	information	admin	edit	User admin changed local-user jack from GUI(172.22.10.90)
12	2015-12-01	16:34:45	information	admin	delete	User admin deleted local-user tom from GUI(172.22.10.90)
11	2015-12-01	16:34:42	information	admin	add	User admin added local-user jack from GUI(172.22.10.90)
10	2015-12-01	16:34:31	information	admin	add	User admin added local-user tom from GUI(172.22.10.90)
9	2015-12-01	16:28:53	information	admin	login	User admin logged in successfully from GUI->HTTP(172.22.10.90)
8	2015-12-01	16:28:07	information	admin	logout	User admin logged out from GUI->HTTP(172.22.10.90)
7	2015-12-01	16:25:56	information	admin	login	User admin logged in successfully from GUI->HTTP(172.22.10.90)
6	2015-12-01	16:24:00	information	admin	logout	User admin logged out from GUI->HTTP(172.22.10.90)
5	2015-12-01	16:22:33	information	admin	login	User admin logged in successfully from GUI->HTTP(172.22.10.90)
4	2015-12-01	16:21:16	information	admin	logout	User admin logged out from GUI->HTTP(172.22.10.90)
3	2015-12-01	16:16:18	information	admin	login	User admin logged in successfully from GUI->HTTP(172.22.10.90)
2	2015-12-01	16:16:16	information	admin	logout	User admin logged out from GUI->HTTP(172.22.10.90)
1	2015-12-01	16:06:11	information	admin	login	User admin logged in successfully from GUI->HTTP(172.22.10.90)

Add, configure, and provision devices (Device Manager tab)

Add a group

Prepare to add devices to your FortiWeb Manager by creating device groups. These groups allow you to organize your devices in the navigation tree.

To add a group

On the Device Manager tab, click **Add Group** and then complete the following settings:

Name	The name for the FortiWeb Manager device group.
Description	An optional description for the group (for example, a description of its geographic location).

Add a device

Before you add a FortiWeb device to your FortiWeb Manager configuration, ensure that it has the following local configuration:

- The FortiWeb is running the required firmware version. See Software requirements on page 8.
- A network interface that is configured with an IP address that FortiWeb Manager can reach and allows HTTPS connections. (FortiWeb Manager uses HTTPS port 90 to communicate with devices.)
- An administrator account that can access the configuration areas you want to edit using FortiWeb Manager. This account can be `admin`.

Because you specify the group that a device belongs to when you add a device, it is helpful to create the group you want the device to belong to before you add the device.

To add a device

On the Device Manager tab, click **Add Device** and then complete the following settings:

Name	The name for the device in the FortiWeb Manager configuration.
IP Address	The IP address that FortiWeb Manager can use to to communicate with the device.
User Name	The name of an administrator account on the device that can access the configuration areas you want to edit using FortiWeb Manager.

Password	The password that corresponds to the specified **User Name**.
Add to Groups	• **None** – The device does not belong to a group. • **Specific** – The device belongs to the FortiWeb Manager group specified by **Group**.
Group	The FortiWeb Manager group the device belongs to. Available only if **Add to Groups** is **Specific**.
Description	An optional description for the device (for example, a description of its physical location).

Access device configuration

Use the **Devices & Groups** navigation menu to access the configuration settings for an individual device. You can also use this menu to access the status dashboard information and other tasks you perform using the FortiWeb web UI.

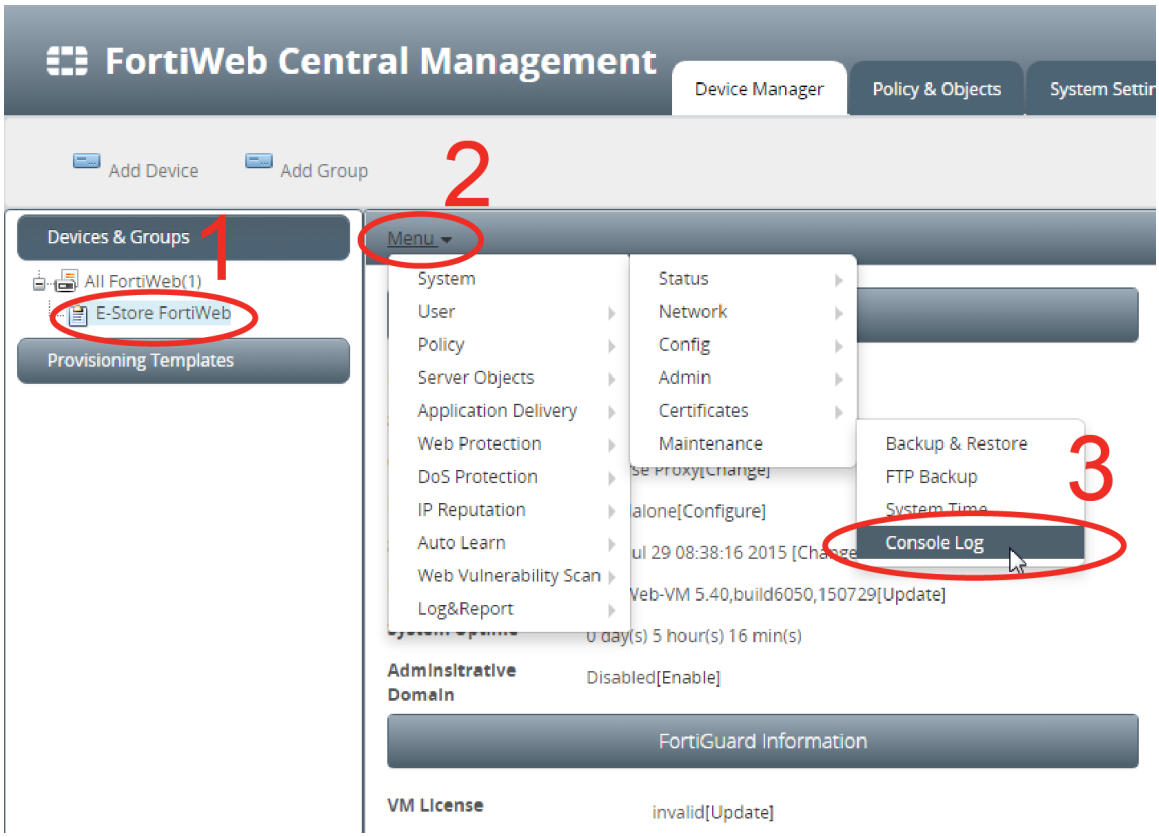
FortiWeb Manager applies any changes you make to the device configuration immediately. And if another administrator makes changes to the device you are viewing, FortiWeb Manager displays those changes the next time it refreshes the view (for example, when you select a different configuration element.)

To access individual configuration settings for a device

1. Under **Devices & Groups**, expand the **All FortiWeb** item.
2. In the list of devices, click the appropriate device.

   By default, the content pane displays the status dashboard for the device.

3. In the content pane toolbar, click **Menu**, and then use the menu to select the configuration item you want to view or edit.



Creating and applying provisioning templates

The **Provisioning Templates** navigation menu allows you to add, edit, and apply sets of settings that you use when you initially set up a FortiWeb.

You can edit a template at any time, but FortiWeb Manager does not apply the changes to a device until you apply or reapply the template.

To apply the template settings to a FortiWeb, you first use the **Add Device** option to add it to the device list.

When you apply a template to a device, FortiWeb Manager saves the current system configuration values. If it is unable to apply one or more settings from the template, it restores the values it saved. If successfully applies the template, it saves the original values as a file you can download or restore using the Templates Assign log (see Templates Assign on page 15).

For descriptions of the template configuration settings, see the *FortiWeb Administration Guide*.

Task	Instructions
Create a new system template	1. Under **Provisioning Templates**, right-click any item, and then click **Create New**. 2. Enter a name and optional description, and then click **OK**. 3. For each widget, enter appropriate values, and then click **Apply**. **Apply** saves values in the template. To apply it to a device, you apply the template to the device.
Add or update settings in the template	Under **Provisioning Templates**, click the appropriate template, add or edit settings in the appropriate widget, and then click **Apply**.
Apply system template settings to a FortiWeb	1. Under **Provisioning Templates**, right-click the template, then click **Assign Device**. 2. For **Devices**, select the device you want to apply the template to, and then click **OK**.
Delete a system template	Under **Provisioning Templates**, right-click the template, then click **Delete**.
Revert to the original configuration	Go to **Logs > Template Assign**, and for the log item for the template assignment, click **Revert**. For more information, see Templates Assign on page 15.

Create and install reusable server policies (Policy & Objects tab)

The **Policy & Objects** tab allows you to create, manage and apply the following reusable configuration resources:

- Shared configuration objects such as virtual servers, server pools, and web protection profiles. Server policies in packages reference these objects in server policies, either directly or through other objects. You can reference each configuration object in multiple policies and objects. You can't delete an object if it is referenced by a policy or another object.
- Policy packages that contain one or more server policies and apply to a specified operating mode. Thses server policies use the predefined configuration objects.

Package installation

When your policy package is complete, you can install it on a FortiWeb from the FortiWeb Manager device list. For each policy package, FortiWeb Manager maintains a list of the installation instances.

When you install a policy package on a device, FortiWeb Manager saves the current values of all server policies and related objects on the target appliance. If FortiWeb Manager successfully installs the package, it saves the original configuration as a file you can download or restore using the Package Install log (see Package Install on page 15). If the installation is unsuccessful, it restores the values it saved.

FortiWeb Manager only installs the reusable configuration objects that are referenced by policies in the package. However, to avoid possible conflicts, it deletes all configuration objects from the target FortiWeb, even if they are not referenced by a policy.

Editing packages

You can edit a policy package at any time, but FortiWeb Manager does not apply the changes until you install or reinstall the package.

Task	Instructions
Create configuration objects	1. On the Policy & Objects tab, under **Objects**, expand the navigation tree items until the type of object you want to create is displayed, and then click it. 2. In the content pane, click **Create New**. 3. Complete the settings for the new object, and then click **OK**.

Task	Instructions
Create a new policy package	1. Click **Policy Package > Create New**. 2. Enter a name for the package, select an operating mode, and then click **Apply**.
Add a policy to a policy package	1. Ensure that you have added the configuration objects that the policy uses to the list of objects. 2. Under **Policy Package**, select the package to add the policy to. 3. In the Policy & Objects toolbar, click **Policy > Create New**. 4. Complete the settings for the policy, and then click **Apply**.
Install a policy package on a FortiWeb	1. Under **Policy Package**, right-click the package to install, and then click **Install Wizard**. 2. Select the appropriate device, enter an optional comment, and then **OK**.
Revert to the original configuration	Go to **Logs > Package Install**, and for the package installation log item, click **Revert**. For more information, see Package Install on page 15.

High Performance Network Security